MULTI-FACTOR AUTHENTICATION (MFA) POLICY – AFINCE

Effective Date: April 14, 2026

1. PURPOSE
This policy defines the use of multi-factor authentication (MFA) to protect access to critical systems that store or process sensitive financial data.

2. SCOPE
This policy applies to all administrative and production systems, including cloud infrastructure, backend services, and third-party integrations.

3. MFA REQUIREMENTS
- MFA is enabled for all administrative access to critical systems.
- MFA methods include email verification, SMS-based codes, and device-based authentication.
- Access to cloud platforms (e.g., Google Cloud / Firebase) requires secure authentication with MFA enabled.

4. ACCESS CONTROL
- Only authorized personnel may access production systems.
- MFA is required before accessing sensitive data environments.
- Sessions are monitored and restricted based on authentication status.

5. SECURITY MEASURES
- Strong passwords are enforced.
- HTTPS encryption is used for all communications.
- Access logs and authentication attempts are monitored.

6. THIRD-PARTY PROVIDERS
- Trusted providers (e.g., Google Cloud, Plaid) enforce additional security layers, including MFA where applicable.

7. CONTINUOUS IMPROVEMENT
Afince continuously evaluates and enhances authentication mechanisms to improve security and reduce risk.

8. CONTACT
Email: support@afince.com
Website: https://afince.com